Fastly & PerimeterX

Protect your website, mobile apps, and APIs from malicious bots

Fastly and PerimeterX: a better bot mitigation solution

With malicious bot activity on the rise, and becoming more sophisticated, effective bot mitigation needs to start closer to the source of the problem. Fastly has partnered with PerimeterX to create a predictive behavior-based bot detection and mitigation solution at the network edge, that scales instantly and does not impact origin performance.

The Fastly enabled PerimeterX Bot Defender™ solution protects your site from a range of malicious bots, spanning basic scripts to more sophisticated bots that are adept at operating under cover of legitimate users. PerimeterX Bot Defender is the only solution capable of detecting highly sophisticated man-in-the-browser bots which reside inside infected browsers and control users' machines or use advanced browser automation tools. Unlike other solutions, Fastly and PerimeterX enable you to protect both cached content and origin content, so you can keep more content in cache without the risk of bot abuse.

An average of 40% of all login attempts are malicious in nature, and can be as high as 90% during an attack.

PerimeterX, October 2018

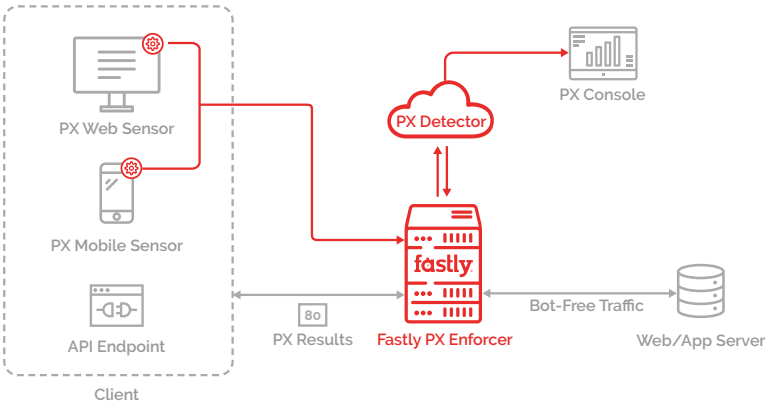
How does it work?

The solution begins with PerimeterX Sensor, which is deployed by placing a snippet of JavaScript on your site or implementing an SDK in your mobile app. This sensor allows PerimeterX to gather behavioral and statistical data, which is analyzed in real time to generate a risk score for a client. PerimeterX collects hundreds of network, browser/device, and user indicators and evaluates them to determine if a request is from a human or bot. The platform continuously autotunes itself to improve bot detection accuracy.

When a request is made to your site or app, Fastly caches and delivers the PerimeterX Sensor, in addition to the requested content. Based on the PerimeterX risk scores set for each client, Fastly can either allow or deny access to your backend server. Additional levels of control can also be applied before granting access such as block, challenge, rate limit, and predict. You can also set additional header values for further client isolation and tracking. Fastly and PerimeterX provide real-time visibility and reporting, empowering you to refine policies on the fly.

If the client doesn't allow PerimeterX to set a cookie, it's a good indicator that the request is coming from a bot and not a human. In this case, Fastly can merge additional header information, fetched through a dedicated API with PerimeterX, to validate the client and block abuse.

By extending your abuse policy to the network edge, you can significantly reduce malicious origin traffic, saving on backend server resources and reducing abuse.



Fastly and PerimeterX Bot Defender

Protect web, mobile apps, and APIs from:

- Content/price scraping
- Account takeover
- Fake user account creation
- Carding
- Marketing/click fraud
- Checkout abuse/scalping
- Layer 7 DDoS attacks

Business benefits

Prevent account takeover

Bot networks often use lists of common and stolen user and password combinations, attempting to log into client accounts. Those accounts contain sensitive information which might be sold or abused.

Protect marketing budget

With affiliate fraud, malicious bots collect referral fees for customers who visit your website directly without being referred by an affiliate. Ad click fraud acquires fake traffic through bots clicking on online ads. These activities can cause you to allocate marketing budgets based on fraudulent campaigns, thereby negatively impacting your return on investment. Bots imitating human behavior can heavily skew your analytics, hide actual trends and obfuscate your actual user behavior.

Control pricing & content strategy

- **Price Scraping –** Advanced bots can create fake accounts and perform "price intelligence" services to help competing websites, selling similar products, to be slightly cheaper and appear higher in various price comparison engines.
- **Scalping –** Bots can mimic human behavior, buying from websites that sell tickets or limited stock merchandise and selling them at a much higher price. This activity skews the supply and demand balance, making it hard to control the buyer's experience.

Block Layer 7 DDoS attacks

The newest generation of bots can imitate legitimate browser behaviors, making them much harder to detect at layer 7. PerimeterX Bot Defender can differentiate between a real user and a man-in-the-browser bot. Fastly's enforcement capabilities can then block this advanced threat vector at the CDN edge, protecting your website from disruptive DDoS attacks.

Getting started

For more information, on Fastly and PerimeterX Bot Defender, please contact us at PerimeterX@fastly.com. We would be happy to set you up with a trial account to explore the benefits of this joint offering.